REMARKS

The above amendment with the following remarks is submitted to be fully responsive to the Office Action of August 14, 2006. Reconsideration of this application in light of the amendment and the allowance of this application are respectfully requested.

Claims 31, 33-36, 38-61, 63-66 and 68-91 were pending in the present application prior to the above amendment. In response to the Office Action, claims 31, 33-35, 54, 61, 63-65, and 84 are amended, and claims 36 and 66 are canceled. Therefore, claims 31, 33-35, 38-61, 63-65, and 68-91 are still pending in the present application and are believed to be in proper condition for allowance.

Claims 31, 33-36, 41-54, 56-61, 63-66, 71-84, and 86-91 are rejected under 35 U.S.C. 103(a) as being unpatentable over Comay (U.S. Patent No. 6,363,489) in view of Pearson (U.S. Patent No. 6,990,591). Claims 38-40, 55, 68-70, and 85 are rejected under 35 U.S.C. 103(a) as being unpatentable over Comay in view of Pearson, in further view of Lyle (U.S. Patent No. 6,886,102). Applicant respectfully requests these rejections be withdrawn.

In amended independent claim 31, Applicant recites:

> A system for protecting a distributed network from unauthorized access, the system comprising:
>
> an intrusion detection system, including:
>
> an intrusion detection module, and
>
> a communications management module coupled to the intrusion detection module; and
>
> intrusion analysis system coupled to the intrusion detection system, and including:
>
> an intrusion analysis module, and
>
> an intrusion reaction coordination module coupled to the intrusion analysis module,
>
> wherein the intrusion detection module detects a possible unauthorized access attempt into or within a distributed network being protected,
>
> the communications management module is coupled to the intrusion analysis module and forwards to the intrusion analysis module information regarding the detected possible unauthorized access attempt,
>
> the intrusion analysis module determines based on the information regarding the detected possible unauthorized access attempt whether or not the detected possible unauthorized access attempt is authorized,
>
> if the intrusion analysis module determines that the detected possible unauthorized access attempt is authorized, the intrusion analysis module forwards, via the communications management module, information to the intrusion detection module that the possible unauthorized access attempt is authorized, and
>
> if the intrusion analysis module determines that the detected possible unauthorized access attempt is not authorized, the intrusion analysis module determines, via the intrusion reaction coordination module, appropriate actions, including forwarding information regarding the detected unauthorized access

attempt to a monitoring center external to the distributed network being protected, and processing information from the monitoring center regarding the detected unauthorized access attempt,

wherein the intrusion analysis system in cooperation with the intrusion detection system enable communications between the monitoring center and an entity attempting the unauthorized access attempt without the entity being made aware that the entity attempting the unauthorized access attempt is communicating with the monitoring center,

wherein the monitoring center sends information to the analysis system and intended for the entity attempting the unauthorized access attempt, the analysis system substitutes origin information of the monitoring center from the received information with origin information of a target of the unauthorized access attempt and forwards the substituted information to the entity attempting the unauthorized access attempt, whereby it appears to the entity attempting the unauthorized access attempt that communications are continuing with the target of the unauthorized access attempt, and

wherein the intrusion analysis system in cooperation with the intrusion detection system engages the entity attempting the unauthorized access attempt to determine the location or origin of the entity attempting the unauthorized access attempt.

Similarly, in amended independent claim 61, Applicant recites:

A method for protecting a distributed network from unauthorized access for use in a system including an intrusion detection system having an intrusion detection module, and a communications management module coupled to the intrusion detection module, and intrusion analysis system coupled to the intrusion detection system, and including an intrusion analysis module, and an intrusion reaction coordination module coupled to the intrusion analysis module, the method comprising:

detecting, by the intrusion detection module, a possible unauthorized access attempt into or within a distributed network being protected;

forwarding, by the communications management module, information regarding the detected possible unauthorized access attempt to the intrusion analysis module;

determining, by the intrusion analysis module, based on the information regarding the detected possible unauthorized access attempt whether or not the detected possible unauthorized access attempt is authorized;

if the intrusion analysis module determines that the detected possible unauthorized access attempt is authorized, forwarding, by the intrusion analysis module, via the communications management module, information to the intrusion detection module that the possible unauthorized access attempt is authorized, and

if the intrusion analysis module determines that the detected possible unauthorized access attempt is not authorized, determining, by the intrusion analysis module, via the intrusion reaction coordination module, appropriate actions, including forwarding information regarding the detected unauthorized access attempt to a monitoring center external to the distributed network being protected, and processing information from the monitoring center regarding the detected unauthorized access attempt,

wherein the intrusion analysis system in cooperation with the intrusion detection system enable communications between the monitoring center and an entity attempting the unauthorized access attempt without the entity being made aware that the entity attempting the unauthorized access attempt is communicating with the monitoring center, and

> wherein the monitoring center sends information to the analysis system and intended for the entity attempting the unauthorized access attempt, the analysis system substitutes origin information of the monitoring center from the received information with origin information of a target of the unauthorized access attempt and forwards the substituted information to the entity attempting the unauthorized access attempt, whereby it appears to the entity attempting the unauthorized access attempt that communications are continuing with the target of the unauthorized access attempt, and
>
> wherein the intrusion analysis system in cooperation with the intrusion detection system engages the entity attempting the unauthorized access attempt to determine the location or origin of the entity attempting the unauthorized access attempt.

The Examiner asserts that Comay teaches the element "wherein the intrusion analysis system in cooperation with the intrusion detection system engages the entity attempting the unauthorized access attempt to determine the location or origin of the entity attempting the unauthorized access attempt" as is recited in independent claims 31 and 61. However, Applicant respectfully submits that Comay does not teach or suggest the element "wherein the intrusion analysis system in cooperation with the intrusion detection system engages the entity attempting the unauthorized access attempt to determine the location or origin of the entity attempting the unauthorized access attempt".

Comay describes an intrusion analysis system that captures information from an intruder, including the source address of unauthorized source 20 (col. 5, lns. 32-35). However, Applicant's invention does not simply capture address information. Instead, Applicant's invention engages the intruder, as is claimed in claims 31 and 61. This is explained in more detail in Applicant's Specification:

> Unauthorized access attempt tracing can be performed, for example, autonomously, i.e., by one or more entities without implementing general surveillance over the internet. In this case, when an unauthorized access attempt is detected and confirmed as hostile act, a concealed program can be embedded in the response to the origin of the unauthorized access attempt. Then, for example, when the hacker receives the target station's response, a concealed program could act as a "worm" within the one or more computers from which the unauthorized access attempt originated. For example, the program, such as a Java® script, or other executable program, could cause the unauthorized access attempting station to validate the hostile attempt and, if the attempt is confirmed, secretly forward the real identification, such as an IP address, to the target station or some other predetermined destination(s).

> In other words, for example, in the case of an HTML page being sent as a response to an unauthorized access attempt, the page can contain an executable program which could be invisible to the hacker. Additionally, a disguised request for confirming hostile intent could be included in such an HTML page. For example, if the target system does not employ a "user ID" feature, a fake request for such a user ID could be made. By the act of attempting to enter a user ID, a hacker confirms they are not familiar with the target system and that they are trying to enter the system in an unauthorized manner. The concealed program could then, for example, be triggered if a hacker enters any user ID. This concealed program could then instruct the hacker's computer, for example, to forward information regarding the hacker to a predetermined destination, such as a pre-programmed IP address. This information could then be forwarded, for example, to a law enforcement or other entity as appropriate. (p. 3, ln. 11 to p. 4, ln. 3).

Thus, Applicant respectfully submits that Comay does not teach or suggest each and every element of claims 31 and 61.

Applicant further submits that neither Pearson nor Lyle teaches or suggests the element "wherein the intrusion analysis system in cooperation with the intrusion detection system engages the entity attempting the unauthorized access attempt to determine the location or origin of the entity attempting the unauthorized access attempt" as disclosed in independent claims 31 and 61.

Pearson teaches an intrusion detector 160 (col. 8, lns. 33-57) but does not teach an intrusion analysis system and does not teach engaging the entity attempting the unauthorized access attempt. Thus, Applicant respectfully submits that Pearson does not teach or suggest each and every element of claims 31 and 61.

Likewise, Lyle teaches an analysis framework in a system that takes responsive action to an incident (Fig. 9, col. 15, ln. 32 to col. 16, ln. 43) but does not teach engaging the entity attempting the unauthorized access attempt. Thus, Applicant respectfully submits that Pearson does not teach or suggest each and every element of claims 31 and 61.

Applicants respectfully submit that neither Comay, Pearson, nor Lyle teach, disclose or suggest the claim limitations of "wherein the intrusion analysis system in cooperation with the intrusion detection system engages the entity attempting the unauthorized access attempt to determine the location or origin of the entity attempting the unauthorized access attempt"

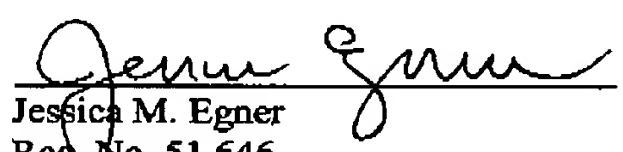
as recited in independent claims 31 and 61, and that neither Comay, Pearson, nor Lyle render claims 31 and 61 unpatentable. Accordingly, in view of the foregoing remarks, the Examiner is respectfully requested to reconsider and withdraw the rejections of claims 31 and 61.

Dependent claims 33-36, 38-60, 63-66 and 68-91 depend from independent claims 31 and 61, and are therefore allowable at least for the aforementioned reasons, and further for the additional features recited.

Conclusion

In view of the foregoing, it is submitted that the present application is in condition for allowance and a notice to that effect is respectfully requested. However, if any issue remains after considering this response, the Examiner is invited to call the undersigned to expedite the prosecution and work out any such issue by telephone.

Respectfully submitted,



Jessica M. Egner
Reg. No. 51,646

NIXON PEABODY LLP
401 9th Street, N.W., Suite 900
Washington, D.C. 20004-2128
(202) 585-8000
(202) 585-8080 (Fax)
Customer No. 22204

Dated: April 13, 2007